Journal of Pure and Applied Algebra 216 (2012) 1528–1532

Contents lists available at SciVerse ScienceDirect

Journal of Pure and Applied Algebra

journal homepage: www.elsevier.com/locate/jpaa

A family of maximal hyperelliptic curves

Saeed Tafazolian *

School of Mathematics, Institute for Research in Fundamental Sciences (IPM), P. O. Box: 19395-5746, Tehran, Iran
Department of Mathematics, Institute for Advanced Studies in Basic Sciences (IASBS), P. O. Box 45195-1159, Zanjan, Iran

ARTICLE INFO

Article history:
Received 20 January 2011
Received in revised form 13 December 2011
Available online 16 February 2012
Communicated by A.V. Geramita

MSC: 11G20; 11M38; 14G15; 14H25

ABSTRACT

The aim of this paper is to give a characterization of maximal hyperelliptic curves $\mathcal{C}$ over a finite field $\mathbb{F}_{q^2}$ given by the equation $y^2 = x^m + 1$.

1. Introduction

Let $\mathcal{C}$ be a (projective, non-singular and geometrically irreducible) curve of genus g defined over a finite field $\mathbb{F}_q$ with q elements. We know after A. Weil that the number of $\mathbb{F}_q$-rational points of a curve of genus g defined over $\mathbb{F}_q$ satisfies the following limitations:

$$q + 1 - 2g\sqrt{q} \leq \#\mathcal{C}(\mathbb{F}_q) \leq 1 + q + 2g\sqrt{q},$$

where $\mathcal{C}(\mathbb{F}_q)$ denotes the set of $\mathbb{F}_q$-rational points of the curve $\mathcal{C}$.

Here we will be interested in maximal (resp. minimal) curves over $\mathbb{F}_{q^2}$, that is, we will consider curves $\mathcal{C}$ attaining Hasse–Weil's upper (resp. lower) bound:

$$\#\mathcal{C}(\mathbb{F}_{q^2}) = q^2 + 1 + 2gq \quad (\text{resp. } q^2 + 1 - 2gq).$$

In this paper, we consider maximal hyperelliptic curves over a finite field with q^2 elements of characteristic $p > 2$. Let $\mathcal{C}$ be a hyperelliptic curve over $\mathbb{F}_{q^2}$ of genus g. Then $\mathcal{C}$ can be defined by an affine equation of the form

$$y^2 = f(x),$$

where $f(x)$ is a polynomial over $\mathbb{F}_{q^2}$ of degree $2g + 1$ or $2g + 2$, without multiple roots.

In this work, we consider the hyperelliptic curve $\mathcal{C}$ given by the equation $y^2 = x^m + 1$ over $\mathbb{F}_{q^2}$. We are going to determine when this curve is maximal over $\mathbb{F}_{q^2}$. In fact, we show the following theorem.

Theorem 1. *Suppose q is an odd prime power and let m be a positive integer such that $\gcd(q, m) = 1$. The smooth complete hyperelliptic curve $\mathcal{C}$ corresponding to*

$$y^2 = x^m + 1$$

is maximal over $\mathbb{F}_{q^2}$ if and only if m divides $q + 1$.

This generalizes Propositions 2, 3 and 5 in [5], which deal with the particular cases $m = 7$, 8 and 12.

* Correspondence to: Institute for Research in Fundamental Sciences (IPM), P. O. Box: 19395-5746, Tehran, Iran.
E-mail address: tafazolian@iasbs.ac.ir.

0022-4049/$ – see front matter
doi:10.1016/j.jpaa.2012.01.019

2. Preliminaries

Before giving the proof of the main result, we need to recall some properties of maximal curves and also some tools (which include the Hasse–Witt matrix of curves and Weierstrass point theory) that are used in the proof.

Let $\mathcal{C}$ be a curve of genus $g > 0$ over the finite field $k = \mathbb{F}_q$ of characteristic p with q elements. The *zeta function* of $\mathcal{C}$ is a rational function of the form

$$Z(\mathcal{C}/k) = \frac{L(t)}{(1-t)(1-qt)},$$

where $L(t) \in \mathbb{Z}[t]$ is a polynomial of degree $2g$ with integral coefficients (see [10, Chapter V]). We call this polynomial the *L-polynomial* of $\mathcal{C}$ over k.

We recall the following fact about maximal curves which can be deduced by extending the argument on p. 182 of [10].

Proposition 2. *Suppose q is square. For a smooth projective curve $\mathcal{C}$ of genus g, defined over $k = \mathbb{F}_q$, the following conditions are equivalent.*

- *$\mathcal{C}$ is maximal (resp. minimal) over $\mathbb{F}_q$.*
- *$L(t) = (1 + \sqrt{q}t)^{2g}$ (resp. $L(t) = (1 - \sqrt{q}t)^{2g}$).*

A well-known example of a maximal curve over $\mathbb{F}_{q^2}$ is the Hermitian curve $\mathcal{H}$; it is defined by $x^{q+1} + y^{q+1} = 1$ (see [10, Example VI.3.6]). If we choose $\xi \in \mathbb{F}_{q^2}$ with $\xi^{q+1} = -1$ and set $x_1 := \xi x$, then the curve $y^{q+1} = x_1^{q+1} + 1$ is isomorphic over $\mathbb{F}_{q^2}$ to $\mathcal{H}$. In this paper, we will use this later equation of the Hermitian curve, i.e.,

$$\mathcal{H} : y^{q+1} = x^{q+1} + 1.$$

Remark 3. As Serre has shown, if there is a morphism defined over the field k between two curves $f : \mathcal{C} \longrightarrow \mathcal{D}$, then the L-polynomial of $\mathcal{D}$ divides the one of $\mathcal{C}$. Hence a subcover $\mathcal{D}$ of a maximal curve $\mathcal{C}$ is also maximal (see [4]). So one way to construct explicit maximal curves is to find equations for subcovers of the Hermitian curve (see [2]).

Definition. The *p-rank* of an abelian variety $\mathcal{A}/k$, denoted by $\sigma(\mathcal{A})$, is the p-rank of the group $\mathcal{A}(\bar{k})$ or, equivalently, the dimension of $\mathcal{A}(k)$ as an $\mathbb{F}_p$-vector space. The *p-rank* $\sigma(\mathcal{C})$ of a curve $\mathcal{C}/k$ is the p-rank of its Jacobian. We also call it the *Hasse–Witt invariant* of the curve.

If we have the L-polynomial of a curve $\mathcal{C}$, we can use the following result to determine its Hasse–Witt invariant (see [9]).

Proposition 4. *Let $\mathcal{C}$ be a curve defined over $k = \mathbb{F}_q$. If the L-polynomial of $\mathcal{C}$ is of the form $L = 1 + a_1 t + \cdots + a_{2g-1}t^{2g-1} + q^g t^{2g}$, then the Hasse–Witt invariant satisfies*

$$\sigma(\mathcal{C}) = \max\{i \mid a_i \not\equiv 0 \pmod{p}\}.$$

Corollary 5. *If a curve $\mathcal{C}$ is maximal (or minimal) over a finite field, then the Hasse–Witt invariant satisfies $\sigma(\mathcal{C}) = 0$.*

Proof. This follows from the above proposition and Proposition 2. □

In the following lemma we recall the relation between maximality and minimality of a curve over a constant field extension.

Lemma 6. *Let $\mathcal{C}$ be a maximal curve over $\mathbb{F}_{q^2}$. Then $\mathcal{C}$ is maximal (resp. minimal) over the constant field extension $\mathbb{F}_{q^{2r}}$ if r is odd (resp. if r is even).*

Proof. If $L_r(t)$ denotes the L-polynomial of $\mathcal{C}$ over the constant field extension $\mathbb{F}_{q^{2r}}$, then from Proposition 2 and [10, Theorem V.1.15] we obtain that $L_r(t) = (1 - (-q)^r t)^{2g}$. Therefore, the desired result follows from Proposition 2. □

Let $\mathcal{C}$ be a curve defined over a perfect field of characteristic $p > 0$. Let Ω^1 be the sheaf of differential 1-forms on $\mathcal{C}$. Then there exists a canonical $1/p$-linear operator $\mathscr{C} : \Omega^1 \to \Omega^1$, which is the so-called *Cartier operator*.

For a basis $\omega_1, \ldots, \omega_g$ of $H^0(\mathcal{C}, \Omega^1)$ let (a_{ij}) denote the associated matrix of the Cartier operator $\mathscr{C}$, i.e., we have

$$\mathscr{C}(\omega_j) = \sum_{i=1}^{g} a_{ij}\omega_i.$$

The corresponding *Hasse–Witt matrix* $\mathscr{A}(\mathcal{C})$ is obtained by taking p-th powers, i.e., we have

$$\mathscr{A}(\mathcal{C}) = (a_{ij}^p).$$

Remark 7. Because of $1/p$-linearity, the operator $\mathscr{C}^n$ is represented with respect to the basis $\omega_1, \ldots, \omega_g$ by the product of matrices below:

$$(a_{ij}^{1/p^{n-1}}) \ldots (a_{ij}^{1/p})(a_{ij}).$$

By raising the coefficients of this matrix to p^n-th powers we get the matrix

$$\mathscr{A}(\mathcal{C})^{[n]} = (a_{ij}^{p})(a_{ij}^{p^2}) \dots (a_{ij}^{p^n}).$$

It is remarkable that if $n \geq g$, then the rank of the matrix $\mathscr{A}(\mathcal{C})^{[n]}$ does not depend on n and it is equal to the Hasse–Witt invariant of $\mathcal{C}$ (see [8, Sections 9–11]). Note that this formula also applies when $g = 1$.

From [12] we can determine the Hasse–Witt matrix of an elliptic or hyperelliptic curve $y^2 = f(x)$ as follows.

Let $\omega = (\omega_1, \dots, \omega_g)$ be the usual basis of $H^0(\mathcal{C}, \Omega^1)$ given by $\omega_i = \frac{x^{i-1}dx}{y}$, $1 \leq i \leq g$. Since $\mathscr{C}(\omega_i) = \frac{1}{y}\mathscr{C}(y^{p-1}x^{i-1}dx) = \frac{1}{y}\mathscr{C}(f(x)^{(p-1)/2}x^{i-1}dx)$, it follows easily from properties of the Cartier operator that

$$M := \mathscr{A}(\mathcal{C}) = \begin{pmatrix} c_{p-1} & c_{p-2} & \dots & c_{p-g} \\ c_{2p-1} & c_{2p-2} & \dots & c_{2p-g} \\ \vdots & & \dots & \vdots \\ c_{gp-1} & c_{gp-2} & \dots & c_{gp-g} \end{pmatrix},$$

where the coefficients $c_j \in k$ are the coefficients of the polynomial $f(x)^{(p-1)/2}$. Note that this argument shows that the formula also holds when the degree of $f(x)$ is even, not just when $\deg f(x) = 2g + 1$ as in [12].

Here we review also some results about the theory of Weierstrass points in positive characteristic (see [7]). We use the following terminology and notations.

- The symbol "$\sim$" denotes linear equivalence of divisors.
- For $P \in \mathcal{C}$, $m_i = m_i(P)$ denotes the i-th non-gap at P, with $m_0(P) := 0$, and $H(P) := \{m_i(P) : i \geq 0\}$. We recall that an integer $m > 0$ is a non-gap of P if there is a rational function f on $\mathcal{C}$ such that its pole-divisor $(f)_\infty$ is mP.

From Lemma 1 of [6] we have the following proposition.

Proposition 8. *Let $\mathcal{C}$ be a maximal curve over $\mathbb{F}_{q^2}$, and let P_0 and P_1 be two rational points. Then*

$$(q + 1)P_0 \sim (q + 1)P_1.$$

In particular we have $q + 1 \in H(P_0)$, i.e., $q + 1$ is a non-gap at a rational point.

The following theorem is crucial for us (see [7, Satz 8]).

Theorem 9. *Let $\mathcal{C}$ be a hyperelliptic curve defined over a perfect field of characteristic p. If P is a point on $\mathcal{C}$, then we have the following.*

- *P is a Weierstrass point if and only if P is a ramification point of the hyperelliptic cover (or, equivalently, P is a fixed point of the hyperelliptic involution).*
- *If P is a non-Weierstrass point on the curve $\mathcal{C}$, then P has gap sequence $1, \dots, g$ and so $H(P) = \{0, g + 1, g + 2, \dots\}$.*

3. The proof of the main result

Now we are able to prove our main result. Note that the first part of the proof is similar to the proof of [1, Theorem 3.1] and Lemma 6.2 is similar to Lemma 4.5 in [3], where a hyperelliptic curve is replaced by a Fermat curve.

Proof of Theorem 1. Suppose first that m divides $q + 1$. Set $a := \frac{q+1}{m}$ and $b := \frac{q+1}{2}$. Consider the following morphism

$$\begin{cases} \mathcal{H} & \to & \mathcal{C} \\ (x, y) & \mapsto & (x^a, y^b). \end{cases}$$

Hence $\mathcal{C}$ is covered by the Hermitian curve $\mathcal{H}$ and Remark 3 implies that $\mathcal{C}$ is maximal over $\mathbb{F}_{q^2}$.

To prove the converse, assume now that $\mathcal{C}$ is maximal and consider the affine equation of the curve $y^2 = x^m + 1$. For $\alpha = 1$ and $\beta = -1$, set $P_\alpha := (0 : \alpha)$ and $P_\beta := (0 : \beta)$. Then $\operatorname{div}(y - \alpha) = mP_\alpha - D_1$ and $\operatorname{div}(y - \beta) = mP_\beta - D_1$ for some positive divisor D_1. Thus

$$mP_\alpha \sim mP_\beta.$$

This implies that m belongs to $H(P_\alpha)$. In addition, it follows from Proposition 8 that

$$dP_\alpha \sim dP_\beta,$$

where $d := \gcd(m, q + 1)$. Thus $d \in H(P_\alpha)$. On the other hand, from Theorem 9 we know that P_α is not a Weierstrass point, and so $H(P_\alpha) = \{0, g + 1, g + 2, \dots\}$.

Now if $m = 2g + 1$, then $H(P_\alpha) = \{0, (m + 1)/2, (m + 3)/2, \dots\}$. Thus $\frac{m+1}{2} \leq d \mid m$, and so it follows that $d = m$, i.e., m divides $q + 1$.

But if $m = 2g + 2$, then $H(P_\alpha) = \{0, m/2, (m + 2)/2, (m + 4)/2, \ldots\}$. It follows that $d = m$ or $d = m/2$ which implies that m divides $2(q + 1)$. In this case, we see that if h is an odd divisor of m, then h is a divisor of $q + 1$. The only situation still to be investigated is the following: $q + 1 = 2^r s$ with s an odd integer and $m = 2^{r+1}s_1$ with s_1 a divisor of s. If such a maximal curve given by $y^2 = x^{2^{r+1}s_1} + 1$ would exist, then from Remark 3 we conclude that the curve $y^2 = x^{2^{r+1}} + 1$ is maximal over $\mathbb{F}_{q^2}$. But this is impossible as shown in the next lemma.

Lemma 10. *Assume that the characteristic p is odd and write $q + 1 = 2^r s$ with s an odd integer. We have $m := 2^{r+1}$. Then the hyperelliptic curve $\mathcal{C}(m)$ given by the equation $y^2 = x^m + 1$ is not maximal over $\mathbb{F}_{q^2}$.*

Proof. Writing $q = p^n$, we consider three cases:

Case $p \equiv 3 \pmod 4$ and n even. In this case, we have $q + 1 = 2s$ with s an odd integer and we must show that the curve $\mathcal{C}(4)$ is not maximal over $\mathbb{F}_{q^2}$. Since 4 is a divisor of $p + 1$, the curve $\mathcal{C}(4)$ is maximal over $\mathbb{F}_{p^2}$. Hence by Lemma 6, $\mathcal{C}(4)$ is minimal over $\mathbb{F}_{q^2}$ because n is even.

Case $p \equiv 3 \pmod 4$ and n odd. In this case, we can write $p = 2^r s_1 - 1$, where s_1 is an odd number.

Here we determine the Hasse–Witt matrix M of the hyperelliptic curve $y^2 = x^m + 1$. Using the above notation, we obtain

$$c_j = \begin{cases} \binom{(p-1)/2}{j/m} & \text{if} \quad m \text{ divides } j \\ 0 & \text{if} \quad m \text{ does not divide } j, \end{cases}$$

where $(x^m + 1)^{(p-1)/2} = \sum_{j=0}^{N} c_j x^j$.

Consider the entries of the matrix M. In this case, it is easy to see that m divides $p - g$ and $gp - 1$, and so m does not divide $p - u$ and $gp - t$ for $1 \le u \le g - 1$ and $2 \le t \le g$ because $g < m$. We can also show that $m = 2^{r+1} = 2g + 2$ does not divide $up - 1$ and $tp - g$ for $1 \le u \le g - 1$ and $2 \le t \le g$. In fact, if u is even, then $up - 1 \equiv -u - 1 \pmod m$ and $up - 1 \equiv 2^r - u - 1 \pmod m$ if u is odd. We have similar result for other numbers.

Set $r_1 := (p - g)/m$ and $r_2 := (gp - 1)/m$. Then the Hasse–Witt matrix of the curve $\mathcal{C}(m)$ have the following form:

$$M = \begin{pmatrix} 0 & 0 & \ldots & 0 & a \\ 0 & * & \ldots & * & 0 \\ \vdots & \vdots & \ldots & \vdots & \vdots \\ 0 & * & \ldots & * & 0 \\ b & 0 & \ldots & 0 & 0 \end{pmatrix},$$

where $a = \binom{(p-1)/2}{r_1} \neq 0$ and $b = \binom{(p-1)/2}{r_2} \neq 0$.

Now in order to determine the Hasse–Witt invariant of the curve $\mathcal{C}(m)$, according to Remark 7 we obtain

$$\mathcal{A}(\mathcal{C})^{[2g]} = \begin{pmatrix} a^\lambda b & 0 & \ldots & 0 & 0 \\ 0 & * & \ldots & * & 0 \\ \vdots & \vdots & \ldots & \vdots & \vdots \\ 0 & * & \ldots & * & 0 \\ 0 & 0 & \ldots & 0 & b^\lambda a \end{pmatrix},$$

where λ is an integer. Hence the rank of the matrix $\mathcal{A}(\mathcal{C})^{[2g]}$ is at least two, and so the Hasse–Witt invariant of the curve $\mathcal{C}(m)$ cannot be zero because of Remark 7. By Corollary 5, this means that the curve $\mathcal{C}(m)$ is not a maximal curve.

Case $p \equiv 1 \pmod 4$. In this case, we have $q + 1 = 2s$ with s an odd integer. So we must show that the curve $\mathcal{C}(4)$ is not maximal over $\mathbb{F}_{q^2}$. But, it is easy to show that the curve $\mathcal{C}(4)$ with $p \equiv 1 \pmod 4$ is an ordinary elliptic curve and so it is not maximal. In fact, according to the previous case we obtain $M = [\binom{(p-1)/2}{r'}] \neq 0$, where $p - 1 = 4r'$. Therefore we conclude that the Hasse–Witt invariant of the curve $\mathcal{C}(4)$ is not zero, and so by Corollary 5 the curve $\mathcal{C}(4)$ is not maximal. This completes the proofs of Lemma 10 and Theorem 1. □

Remark 11. Assume that $q = p$ is a prime number. If the curve $\mathcal{C}$ given by the equation $y^2 = x^{2g+1} + 1$ is maximal over $\mathbb{F}_{p^2}$, then [3, Theorem 3.3] implies that the Hasse–Witt matrix of $\mathcal{C}$ is zero. Hence from [11, Theorem 1] we get that $m = 2g + 1$ is a divisor of $p + 1$. The above theorem generalizes this result.

Remark 12. Theorem 1 shows that the curve $y^2 = x^m + 1$ is maximal over $\mathbb{F}_{q^2}$ if and only if it is covered by the Hermitian curve $\mathcal{H}$ over $\mathbb{F}_{q^2}$.

Acknowledgements

I express my deep gratitude to the anonymous referee for his/her valuable comments and suggestions which led to fill all the gaps in the proof of Theorem 1, to find correct references for many assertions and to improve the exposition. Also I thank Arnaldo Garcia for reading this paper and the comments which led to improvement of the presentation. The author was in part supported by a grant from IPM (No. 90140131).

References

[1] A. Aguglia, G. Korchmáros, F. Torres, Plane maximal curves, Acta Arith. 98 (2001) 165–179.
[2] A. Garcia, H. Stichtenoth, C.P. Xing, On subfields of Hermitian function fields, Composito Math. 120 (2000) 137–170.
[3] A. Garcia, S. Tafazolian, Certain maximal curves and Cartier operators, Acta Arith. 135 (2008) 199–218.
[4] G. Lachaud, Sommes d'Eisenstein et nombre de points de certaines courbes algébriques sur les corps finis, C. R. Acad. Sci. Paris Sér. I Math. 305 (1987) 729–732.
[5] T. Kodama, J. Top, T. Washio, Maximal hyperelliptic curves of genus three, Finite Fields Appl. 15 (2009) 392–403.
[6] H-G. Rück, H. Stichtenoth, A characterization of Hermitian function fields over finite fields, J. Reine Angew. Math. 457 (1994) 185–188.
[7] F.K Schmidt, Zur arithmetischen Theorie der algebraischen Funktionen II. Allgemeine Theorie der Weierstraßpunkte, Math. Z. 45 (1939) 75–96.
[8] J.P. Serre, Sur la topologie des variétés algébriques en caractéristique p, Symp. Int. Top. Alg., Mexico (1958) 24–53. *Œuvres/Collected Papers I*, pp. 501–530.
[9] H. Stichtenoth, Die Hasse–Witt Invariante eines Kongruenzfunktionenkörpers, Arch. Math. 33 (1979/80) 357–360.
[10] H. Stichtenoth, Algebraic function fields and codes, Universitext, Springer-Verlag, Berlin, Heidelberg, 1993.
[11] R. Valentini, Hyperelliptic curves with zero Hasse–Witt matrix, Manuscripta Math. 86 (1995) 185–194.
[12] N. Yui, On the Jacobian varieties of hyperelliptic curves over fields of characteristic $p > 2$, J. Algebra 52 (1978) 378–410.